

On the Griesmer bound for nonlinear codes

Emanuele Bellini¹, Eleonora Guerrini², Alessio Meneghetti³, and Massimiliano Sala³

¹ Telsy S.p.A., Italy

eemanuele.bellini@gmail.com

² LIRMM, Université de Montpellier 2, France

guerrini@lirmm.fr

³ University of Trento, Italy

almenegh@gmail.com

⁴ University of Trento, Italy

maxsalacodes@gmail.com

Abstract. Most bounds on the size of codes hold for any code, whether linear or nonlinear. Notably, the Griesmer bound, holds only in the linear case. In this paper we characterize a family of systematic nonlinear codes for which the Griesmer bound holds. Moreover, we show that the Griesmer bound does not necessarily hold for a systematic code by showing explicit counterexamples. On the other hand, we are also able to provide (weaker) versions of the Griesmer bound holding for all systematic codes.

1 Introduction

We consider codes over a finite field \mathbb{F}_q of length n , with M codewords, and distance d . A code C with such parameters is denoted as an $(n, M, d)_q$ -code.

Definition 1. An $(n, q^k, d)_q$ -systematic code C is the image of a map $F : (\mathbb{F}_q)^k \rightarrow (\mathbb{F}_q)^n$, $n \geq k$, s.t. a vector $x = (x_1, \dots, x_k) \in (\mathbb{F}_q)^k$ is mapped to a vector

$$(x_1, \dots, x_k, f_{k+1}(x), \dots, f_n(x)) \in (\mathbb{F}_q)^n,$$

where $f_i, i = k+1, \dots, n$ are maps from $(\mathbb{F}_q)^k$ to \mathbb{F}_q . We refer to k as the dimension of C . The coordinates from 1 to k are called systematic, while those from $k+1$ to n are called non-systematic.

If the maps f_i are all linear, then the systematic code C is a subspace of dimension k of $(\mathbb{F}_q)^n$ and we say it is a $[n, k, d]_q$ -linear code. A nonlinear code is a code which is not necessarily linear or systematic.

We denote with $\text{len}(C)$, $\text{dim}(C)$, $d(C)$, respectively, the length, the dimension (when defined) and the minimum distance of a code C .

A central problem of coding theory is to determine the minimum value of n , for which an $(n, M, d)_q$ -code or an $[n, k, d]_q$ -linear code exists. We denote by $N_q(M, d)$ the minimum length of a nonlinear code over \mathbb{F}_q , with M codewords and distance d . We denote by $S_q(k, d)$ the same value in the case of a systematic code of dimension k , while we use $L_q(k, d)$ in the case of a linear code of dimension k . Observe that

$$N_q(q^k, d) \leq S_q(k, d) \leq L_q(k, d).$$

A well-known lower bound for $L_q(k, d)$ is

Theorem 1 (Griesmer bound). *All $[n, k, d]_q$ linear codes satisfy the following bound:*

$$n \geq L_q(k, d) \geq g_q(k, d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \quad (1)$$

The Griesmer bound, which can be seen as an extension of the Singleton bound ($n \geq d + k - 1$) [HP03] (Section 2.4) in the linear case, has been introduced by Griesmer [Gri60] in the case of binary linear codes and then generalized by Solomon and Stiffler [SS65] in the case of q -ary linear codes.

It is known that the Griesmer bound is not sharp [Mar96], [Van80], [Mar97].

Important examples of linear codes meeting the Griesmer bound are the simplex code [HP03] (Section 1.8) and the $[5, 6, 11]_3$ Golay code [HP03] (Section 1.9), [Gol49].

Many authors such as [Hel81], [HH93], [Tam84], [Mar97], and [Kle04], have characterized classes of linear codes meeting the Griesmer bound. In particular, finite projective geometries play an important role in the study of these codes. For example in [Hel92], [Ham93] and [Tam93] minihypers and maxhypers are used to characterize linear codes meeting the Griesmer bound. Research has been done also to characterize the codewords of linear codes attaining the Griesmer bound [War98].

Many known bounds on the size of nonlinear codes, for example the Johnson bound ([Joh62], [Joh71], [HP03]), the Elias-Bassalygo bound ([Bas65], [HP03]), the Levenshtein bound ([Lev98]), the Hamming (Sphere Packing) bound, the Singleton bound ([PBH98]), the Plotkin bound ([Plo60], [HP03]), the Zinoviev-Litsyn-Laihonen ([ZL84], [LL98]), the Bellini-Guerrini-Sala ([BGS14]), and the Linear Programming bound ([Del73]), are true for both linear and nonlinear codes.

The proof of the Griesmer bound heavily relies on the linearity of the code and it cannot be applied to all nonlinear codes. In Section 2 we prove that, once q and d have

been chosen, if all nonlinear $(n, q^k, d)_q$ -systematic codes with $k < 1 + \log_q d$ respect the Griesmer bound, then the Griesmer bound holds for all systematic codes with the same q and d . In particular for any q and d only a finite set of (k, n) -pairs has to be analysed in order to prove the bound for all k and n .

Using this result, in Section 3 we characterize several families of systematic codes for which the Griesmer bound holds. In Section 4 we provide (weak) versions of the Griesmer bound, holding for any systematic code. Finally, in Section 5, we show explicit counterexamples of nonlinear codes and systematic codes for which the Griesmer bound does not hold.

2 A sufficient condition to prove the Griesmer bound for systematic codes

The following proposition is well-known, we however provide a sketch of the proof for the particular case in which we will make use of it.

Proposition 1. *Let C be an (n, q^k, d) -systematic code, and C' be the code obtained by shortening C in a systematic coordinate. Then C' is an $(n-1, q^{k-1}, d')$ -systematic code with $d' \geq d$.*

Proof. To obtain C' , consider the code $C'' = \{F(x) \mid x = (0, x_2, \dots, x_k) \in (\mathbb{F}_q)^k\}$, i.e. the subcode of C which is the image of the set of messages whose first coordinate is equal to 0. Then C'' is such that $\dim(C'') = k-1$ and $d(C'') \geq d$. Since, by construction, all codewords have the first coordinate equal to zero, we obtain the code C' by puncturing C'' on the first coordinate, so that $\text{len}(C') = n-1$ and $d' = d(C') = d(C'') \geq d$.

The following lemma is well-known, but we provide a proof because it anticipates our later argument.

Lemma 1. *If $n > k$, then given an (n, q^k, d) -systematic code C , there exists an (n, q^k, \bar{d}) -systematic code \bar{C} for any $1 \leq \bar{d} \leq d$.*

Proof. If $n > k$, we can consider the code C^1 obtained by puncturing C in a non-systematic coordinate. C^1 is an $(n-1, q^k, d^{(1)})$ -systematic code. Of course, either $d^{(1)} = d$ or $d^{(1)} = d-1$.

By puncturing at most $n-k$ coordinates, we will find a code whose distance is 1. Then there must exist an $i \leq n-k$ such that the code C^i , obtained by puncturing C in the last i coordinates, has distance equal to \bar{d} .

Theorem 2. For fixed q and d , if

$$S_q(k, d) \geq g_q(k, d) \quad (2)$$

for all k such that $1 \leq k < 1 + \log_q d$, then (2) holds for any positive k , i.e. the Griesmer bound is true for all the systematic codes over \mathbb{F}_q with minimum distance d .

Proof. It is sufficient to show that if an $(n, q^k, d)_q$ -systematic code not satisfying the Griesmer bound exists, then an $(n', q^{k'}, d)_q$ -systematic code not satisfying the Griesmer bound exists with $k' < 1 + \log_q d$, and $n' > k'$.

For each fixed d, q suppose there exists an $(n, q^k, d)_q$ -systematic code not satisfying the Griesmer bound, i.e., there exists k such that $S_q(k, d) < g_q(k, d)$.

Let us call $\Lambda_{q,d} = \{k \geq 1 \mid S_q(k, d) < g_q(k, d)\}$.

If $\Lambda_{q,d}$ is empty then the Griesmer bound is true for such parameters q, d .

Otherwise there exists a minimum $k' \in \Lambda_{q,d}$ such that $S_q(k', d) < g_q(k', d)$.

In this case we can consider an $(n, q^{k'}, d)_q$ systematic code C not verifying the Griesmer bound, namely $n = S_q(k', d)$. Due to Definition 1, C can be seen as the image of a map

$$F(x) = (x_1, \dots, x_{k'}, f_{k'+1}(x), \dots, f_n(x)),$$

where $x = (x_1, \dots, x_{k'})$. We define a code C' as the image of

$$F(x') = (x_2, \dots, x_{k'}, f_{k'+1}(0, x_2, \dots, x_{k'}), \dots, f_n(0, x_2, \dots, x_{k'}))$$

where $x' = (x_2, \dots, x_{k'})$. Clearly, C' is an $(n-1, q^{k'-1}, d')$ systematic code and $d' \geq d$. Applying Lemma 1 to C' , we can obtain an $(n-1, q^{k'-1}, d)_q$ systematic code \bar{C} . Since k' was the minimum among all the values in $\Lambda_{q,d}$, then the Griesmer bound holds for \bar{C} , and so

$$n-1 \geq g_q(k'-1, d) = \sum_{i=0}^{k'-2} \left\lceil \frac{d}{q^i} \right\rceil. \quad (3)$$

We observe that, if $q^{k'-1} \geq d$, then $\left\lceil \frac{d}{q^{k'-1}} \right\rceil = 1$, so we can rewrite (3) as

$$n \geq \sum_{i=0}^{k'-2} \left\lceil \frac{d}{q^i} \right\rceil + 1 \geq \sum_{i=0}^{k'-2} \left\lceil \frac{d}{q^i} \right\rceil + \left\lceil \frac{d}{q^{k'-1}} \right\rceil = \sum_{i=0}^{k'-1} \left\lceil \frac{d}{q^i} \right\rceil = g_q(k', d)$$

Since we supposed $n < g_q(k', d)$, we have reached a contradiction with the assumption $q^{k'-1} \geq d$. Hence for such d , the minimum k in $\Lambda_{q,d}$ has to satisfy $q^{k-1} < d$, which is equivalent to our claimed expression $k < 1 + \log_q d$.

3 Set of parameters for which the Griesmer bound holds in the nonlinear case

In this section we characterize several sets of parameters (q, d) for which the Griesmer bound holds for systematic codes.

3.1 The case $d \leq 2q$

We use Proposition 2 to prove that all q -ary systematic codes with distance up to $2q$ satisfy the Griesmer bound.

Theorem 3. *If $d \leq 2q$ then $S_q(k, d) \geq g_q(k, d)$.*

Proof. First, consider the case $d \leq q$. By Theorem 2 it is sufficient to show that, fixing q, d , for any n an $(n, q^k, d)_q$ -systematic code with $1 \leq k < 1 + \log_q d$ and $n < g_q(k, d)$ does not exist. If $1 \leq k < 1 + \log_q d$ then $\log_q d \leq \log_q q = 1$, and so k may only be 1. Since $g_q(1, d) = d$ and $n \geq d$, we clearly have that $n \geq g_q(1, d)$.

Now consider the case $q < d \leq 2q$. We use again Theorem 2, i.e. we show that, fixing q, d , then for any n an $(n, q^k, d)_q$ -systematic code with $1 \leq k < 1 + \log_q d$ and $n < g_q(k, d)$ does not exist. Suppose this is not true and let us find a contradiction. If $1 \leq k < 1 + \log_q d$ then $\log_q d \leq \log_q 2q = 1 + \log_q 2$, and so k can only be 1 or 2. We have already seen that if $k = 1$ then $n < g_q(k, d)$ for any n , so suppose $k = 2$. Suppose an $(n, q^2, d)_q$ -systematic code exists with $n < \sum_{i=0}^1 \left\lceil \frac{d}{q^i} \right\rceil = d + 2$. Since by the Singleton bound $n \geq d + k - 1$, then we can only have $n = d + 1$, and therefore the only possible systematic code for which $n < g_q(2, d)$ must have parameter $(d + 1, q^2, d)$, and so it is an MDS code. Let us call C such a code. Being systematic, C is the image of a map $F : (\mathbb{F}_q)^2 \rightarrow (\mathbb{F}_q)^{d+1}$ such that $F(x_1, x_2) = (x_1, x_2, f_3(x_1, x_2), \dots, f_{d+1}(x_1, x_2))$. We can assume $F(0, 0) = (0, \dots, 0)$. Any two codewords which have distance 1 in the two systematic components must have distance at least $d - 1$ in the $d - 1$ non-systematic components. Suppose there exists $\alpha, \beta_1, \beta_2 \in \mathbb{F}_q, \beta_1 \neq \beta_2$ such that for a certain i we have $f_i(\alpha, \beta_1) = f_i(\alpha, \beta_2)$. In this case the distance between $F(\alpha, \beta_1)$ and $F(\alpha, \beta_2)$ is less than d . The same is true if we fix β and we consider α_1 and α_2 . This means that, whenever we fix $x_1 = \alpha$ (respectively $x_2 = \beta$) we need each $f_i(\alpha, x_2)$ (respectively $f_i(x_1, \beta)$) to be a permutation on \mathbb{F}_q . Due to this, for each fixed value $x_1 = \alpha$, there exists a unique value β such that $f_i(\alpha, \beta) = 0$, for all i . Suppose now there exists $i \neq j$ such that $f_i(\alpha, \beta) = f_j(\alpha, \beta) = 0$. In this case the weight of $F(\alpha, \beta)$ is less than d , hence we have a contradiction (we assumed $0 \in C$ and $d(C) = d$). We have obtained that if $f_i(\alpha, \beta) = 0$, then $f_j(\alpha, \beta) \neq 0$ for all $j \neq i$. We recall we have

f_3, \dots, f_{d+1} , and we have already proved that, for each fixed α , there exists β_1 such that $f_3(\alpha, \beta_1) = 0$. Hence if $f_4(\alpha, \beta_1)$ cannot be 0 itself, there must exist another possible value β_2 such that $f_4(\alpha, \beta_2) = 0$. Going on in this way we get a contradiction, in fact the number of f_i is equal to $d - 1$, and for them to be 0 for different non-zero values $\beta_1, \dots, \beta_{d-1}$, we need the field \mathbb{F}_q to contain at least d different elements. Hence we obtain the contradiction $q < d \leq 2q$ (by hypothesis) and $q \geq d$.

3.2 The case $q^{k-1} \mid d$

In this section we make use of the Plotkin bound to prove that there exists particular values of d for which we can apply the Griesmer bound to nonlinear codes.

Theorem 4 (Plotkin bound). *Consider an $(n, M, d)_q$ code, with M being the number of codewords in the code. If $n < \frac{qd}{q-1}$, then $M \leq d/(d - (1 - 1/q)n)$, or equivalently $n \geq d((1 - 1/M)/(1 - 1/q))$.*

Proposition 2. *For $r \geq 1$ it holds $N_q(q^k, q^{k-1}r) \geq g_q(k, q^{k-1}r)$.*

Proof. Suppose there exists an $(n, q^k, q^{k-1}r)_q$ -code C that does not satisfy the Griesmer bound. Hence $n < \sum_{i=0}^{k-1} \left\lceil \frac{q^{k-1}r}{q^i} \right\rceil$. Observe that in this case $\sum_{i=0}^{k-1} \left\lceil \frac{q^{k-1}r}{q^i} \right\rceil = \sum_{i=0}^{k-1} \frac{q^{k-1}r}{q^i} = q^{k-1}r \sum_{i=0}^{k-1} \frac{1}{q^i}$. Since $\sum_{i=0}^{k-1} \frac{1}{q^i} = \frac{1 - \frac{1}{q^k}}{1 - \frac{1}{q}}$, we obtain

$$n < q^{k-1}r \left(\frac{1 - 1/q^k}{1 - 1/q} \right). \quad (4)$$

We also observe that $n < q^{k-1}r \left((1 - 1/q^k)/(1 - 1/q) \right) < q^{k-1}r (1/(1 - 1/q)) = d/(1 - 1/q)$, and we can write this inequality as $n < \frac{dq}{q-1}$, which is the hypothesis for the Plotkin bound. Applying it, we get $q^k \leq \left\lfloor \frac{d}{d - n(1 - 1/q)} \right\rfloor \leq \frac{d}{d - n(1 - 1/q)}$, i.e. $n \geq d \left(\frac{1 - 1/q^k}{1 - 1/q} \right)$, which contradicts equation (4). Hence each $(n, q^k, q^{k-1}r)_q$ -code satisfies the Griesmer bound.

Note that Proposition 2 is not restricted to systematic codes, but it holds for nonlinear codes with at least q^k codewords, as next corollary explains.

Corollary 1. *Let $M \geq q^k$. For $r \geq 1$ it holds $N_q(M, q^{k-1}r) \geq g_q(k, q^{k-1}r)$.*

3.3 The case $d = rq^l, 1 \leq r < q$

Lemma 2. *Let q be fixed, $d = q^l r$ for a certain r such that $1 \leq r < q$ and $l \geq 0$, and let k such that $q^{k-1} \leq d$. Then $N_q(k, d) \geq g_q(k, d)$.*

Proof. Being $1 \leq r < q$, the hypothesis $q^{k-1} \leq d$ is equivalent to $k-1 \leq l$. We use Proposition 4 and we set $h = \min(k-1, l)$, obtaining $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$.

Theorem 5. *Let $1 \leq r < q$ and l a positive integer. Then $S_q(k, q^l r) \geq g_q(k, q^l r)$.*

Proof. To prove that the Griesmer bound is true for these particular choices of d we use Theorem 2, hence we only need to prove that the Griesmer bound is true for all choices of k such that $q^{k-1} \leq d$.

We use now Lemma 2, which ensures that all such codes respect the Griesmer bound.

Corollary 2. *If $q = 2$ then for each positive integer l it holds $S_2(k, 2^l) \geq g_2(k, 2^l)$.*

Proof. It follows directly from Theorem 5.

3.4 The case $d = 2^r - 2^s$

In this section we prove that the Griesmer bound holds for all binary systematic codes whose distance is the difference of two powers of 2. We need the following lemmas.

Lemma 3. *Let r be a positive integer, and let $k \leq r+1$. Then $g_2(k, 2^{r+1}) = 2g_2(k, 2^r)$.*

Proof. The hypothesis $k \leq r+1$ implies that for any $i \leq k-1$, both $\left\lceil \frac{2^{r+1}}{2^i} \right\rceil = \frac{2^{r+1}}{2^i}$ and $\left\lceil \frac{2^r}{2^i} \right\rceil = \frac{2^r}{2^i}$. To prove our claim it is therefore enough to explicit $g_2(k, 2^{r+1})$. Indeed we have

$$g_2(k, 2^{r+1}) = \sum_{i=0}^{k-1} \left\lceil \frac{2^{r+1}}{2^i} \right\rceil = \sum_{i=0}^{k-1} \frac{2^{r+1}}{2^i} = 2 \sum_{i=0}^{k-1} \frac{2^r}{2^i} = 2 \sum_{i=0}^{k-1} \left\lceil \frac{2^r}{2^i} \right\rceil = 2g_2(k, 2^r)$$

Lemma 4. *For each k and d it holds*

$$g_2(k, d+1) = g_2(k, d) + \min(k, l+1), \quad (5)$$

where l is the maximum integer such that 2^l divides d .

Proof. We consider l as in the statement of the lemma, then $d = 2^l r$, where r is odd. We consider first the case $k \leq l+1$. The Griesmer bound for this choice of k and d is

$$g_2(k, d+1) = \sum_{i=0}^{k-1} \left\lceil \frac{2^l r + 1}{2^i} \right\rceil,$$

and we observe that for each i we have

$$\left\lceil \frac{2^l r + 1}{2^i} \right\rceil = \frac{2^l r}{2^i} + \left\lceil \frac{1}{2^i} \right\rceil = \frac{2^l r}{2^i} + 1 = \left\lceil \frac{2^l r}{2^i} \right\rceil + 1.$$

Therefore

$$g_2(k, d+1) = \sum_{i=0}^{k-1} \left(\left\lceil \frac{2^l r}{2^i} \right\rceil + 1 \right) = g_2(k, d) + k. \quad (6)$$

On the other hand, if $k > l+1$ we can split the sum in the following way:

$$g_2(k, d+1) = \left(\sum_{i=0}^l \left\lceil \frac{2^l r + 1}{2^i} \right\rceil \right) + \left(\sum_{i=l+1}^{k-1} \left\lceil \frac{2^l r + 1}{2^i} \right\rceil \right). \quad (7)$$

For the first sum we make use of the same argument as above, while for the second sum we observe that $i > l$, which implies

$$\left\lceil \frac{2^l r + 1}{2^i} \right\rceil = \left\lceil \frac{2^l r}{2^i} \right\rceil.$$

Putting together the two arguments, equation (7) becomes

$$g_2(k, d+1) = \left(\sum_{i=0}^l \left\lceil \frac{2^l r}{2^i} \right\rceil + l + 1 \right) + \left(\sum_{i=l+1}^{k-1} \left\lceil \frac{2^l r}{2^i} \right\rceil \right) = \sum_{i=0}^{k-1} \left\lceil \frac{2^l r}{2^i} \right\rceil + l + 1,$$

and the term on the right-hand side is $g_2(k, d) + l + 1$. Together with (6) this concludes the proof.

Lemma 5. *If $k \geq r$, then $g_2(k, 2^r) < 2^{r+1}$.*

Proof. Due to $k \leq r$, for $i < k$ it holds $\left\lceil \frac{2^r}{2^i} \right\rceil = \frac{2^r}{2^i}$. We can write the Griesmer bound as

$$g_2(k, 2^r) = \sum_{i=0}^{k-1} \frac{2^r}{2^i} = 2^r \sum_{i=0}^{k-1} \frac{1}{2^i} < 2^r \cdot 2.$$

Theorem 6. *Let r and s be two positive integers such that $r > s$, and let $d = 2^r - 2^s$. Then $S_2(k, d) \geq g_2(k, d)$.*

Proof. If $r = s + 1$, then $2^r - 2^s = 2^s$, hence we can apply Corollary 5 and our claim holds. Therefore we can assume $r \geq s + 1$ in the rest of the proof. Let us suppose there exists $s < r$ such that $S_2(k, 2^r - 2^s) < g_2(k, 2^r - 2^s)$, i.e. the Griesmer bound does not hold for some $(n, 2^k, d)_2$ -systematic code C , with $d = 2^r - 2^s$ and $n = S_2(k, d)$. Due to Theorem 2, we can consider the case $k < 1 + \log_2 d$, so we put ourselves in the case $k \leq r$.

We call m the ratio n/d , which in the case of C is

$$m = \frac{S_2(k, 2^r - 2^s)}{2^r - 2^s} \leq \frac{g_2(k, 2^r - 2^s) - 1}{2^r - 2^s}$$

We claim that $m < g_2(k, 2^r)/(2^r)$. First we observe that if $k \leq r$, then

$$\frac{g_2(k, 2^r)}{2^r} = \sum_{i=0}^{k-1} \frac{1}{2^i} = 2 \left(1 - \frac{1}{2^k}\right).$$

We consider now the ratio m :

$$m \leq \frac{g_2(k, 2^r - 2^s) - 1}{2^r - 2^s} = \frac{1}{2^r - 2^s} \sum_{i=0}^{k-1} \left\lceil \frac{2^r - 2^s}{2^i} \right\rceil - \frac{1}{2^r - 2^s} \quad (8)$$

We start from the case $k \leq (s + 1)$, and we can write (8) as

$$m < \frac{1}{2^r - 2^s} \sum_{i=0}^{k-1} \frac{2^r - 2^s}{2^i} = \sum_{i=0}^{k-1} \frac{1}{2^i} = 2 \left(1 - \frac{1}{2^k}\right),$$

so in this case $m < g_2(k, 2^r)/(2^r)$. We consider now the case $k > s + 1$, and we write our claim in the following equivalent way:

$$2^r(g_2(k, 2^r - 2^s) - 1) < (2^r - 2^s)g_2(k, 2^r).$$

Rearranging the terms we obtain

$$2^s g_2(k, 2^r) < 2^r(g_2(k, 2^r) - g_2(k, 2^r - 2^s) + 1), \quad (9)$$

and we focus on the difference $g_2(k, 2^r) - g_2(k, 2^r - 2^s)$. For any d' in the range $2^r - 2^s \leq d' < 2^r$ we can apply Lemma 4, observing that $d' = 2^l r$ where $l \leq s$, and this implies $k > l + 1$. We obtain

$$g_2(k, d' + 1) = g_2(k, d') + l + 1.$$

Applying it for all distances from $2^r - 2^s$ till we reach 2^r we obtain

$$g_2(k, 2^r) - g_2(k, 2^r - 2^s) = 2^{s+1} - 1 \quad (10)$$

We substitute now (10) into (9), which becomes

$$2^s g_2(k, 2^r) < 2^r \cdot 2^{s+1} \quad \Rightarrow \quad g_2(k, 2^r) < 2^{r+1},$$

and this is always true provided $k \leq r$, as shown in Lemma 5.

We now consider the $(tn, 2^k, td)_2$ -systematic code C_t obtained by repeating t times the

code C . We remark that the value m can be thought as the slope of the line $d(C_t) \mapsto \text{len}(C_t)$, and we proved that $m < g_2(k, 2^r)/(2^r)$. On the other hand, since $k \leq r$ we can apply Lemma 3, which ensures that $g_2(k, 2^{r+b}) = 2^b g_2(k, 2^r)$, namely the Griesmer bound computed on the powers of 2 is itself a line, and its slope is strictly greater than m . Due to this we can find a pair (t, b) such that

1. $td > 2^b$,
2. $tn < g_2(k, 2^b)$.

This means that we can find a systematic code with distance $d > 2^b$ and length $n < g_2(k, 2^b)$. We can apply Lemma 1, and find a systematic code with the same length and distance equal to 2^b , which means we have an $(tn, k, 2^b)_2$ -systematic code for which $n < g_2(k, 2^b)$. This however contradicts Corollary 2, hence for each $k \leq r$ we have

$$S_2(k, 2^r - 2^s) \geq g_2(k, 2^r - 2^s).$$

Finally, observe that $k \leq r$ implies $k \leq \log_2(2^r) = \lceil \log_2(2^r - 2^s) \rceil < 1 + \log_2 d$, so we can apply Theorem 2 and conclude.

Corollary 3. *Let r and s two positive integers such that $r > s$, and let $d = 2^r - 1$ or $d = 2^r - 2^s - 1$. Then $S_2(k, d) \geq g_2(k, d)$.*

Proof. We prove it for the case $d = 2^r - 2^s - 1$, the same argument can be applied to the other case by applying Corollary 2 instead of Theorem 6.

Suppose $S_2(k, d) < g_2(k, d)$, i.e. there exists an $(n, k, d)_2$ -systematic code for which

$$n < g_2(k, d). \tag{11}$$

We can extend such code to an $(n+1, k, d+1)_2$ -systematic code C by adding a parity check component to each codeword. C has distance $d(C) = d+1 = 2^r - 2^s$, so we can apply Theorem 6 to it, finding

$$n+1 \geq g_2(k, d+1)$$

Observe that d is odd, so applying Lemma 4 we obtain

$$n+1 \geq g_2(k, d+1) = g_2(k, d) + 1 \quad \Rightarrow \quad n \geq g_2(k, d),$$

which contradicts (11).

4 Versions of the Griesmer bound holding for nonlinear codes

In this section we provide some versions of the Griesmer bound holding for any systematic code.

4.1 An improvement of the Singleton bound

For systematic codes we can improve the Singleton bound as follows.

Proposition 3. *For any k and d it holds*

$$S_2(k, d) \geq k + \left\lceil \frac{3}{2}d \right\rceil - 2.$$

Proof. We will apply the same argument as for the proof of the Griesmer bound, which can be found in [HP03] (Section 2.4).

We consider a binary $(n = S_2(k, d), 2^k, d)_2$ -systematic code C such that $0 \in C$, and a codeword $c \in C$ whose weight is equal to the minimum distance d of the code. We also assume c has weight 1 on its systematic part. The assumptions on C and c are w.l.o.g..

We construct a code C' by puncturing C in all the nonzero coordinates of c . We observe that C' is itself a systematic code, due to the assumptions on c . In particular C' is an $(n - d, 2^{k-1}, d')_2$ -systematic code. We consider now a codeword $u \neq 0$ belonging to C' . There exists a vector $v \in (\mathbb{F}_2)^d$ such that the concatenation $(v|u) \in C$. This means that

$$\begin{cases} w(v|u) = w(v) + w(u) \geq d \\ d(c, v|u) = d - w(v) + w(u) \geq d \end{cases}$$

where $w(u)$ stands for the Hamming weight of u . From the two inequality it follows that

$$w(u) \geq \frac{d}{2}. \quad (12)$$

We observe that (12) is true for all non-zero codewords in C' , so we can choose u to have weight 1 in its systematic part. Therefore the length of u has to be at least

$$\text{len}(u) \geq \frac{d}{2} + k - 2. \quad (13)$$

Since C' is an $(n - d, 2^{k-1}, d')_2$ -systematic code, from (13) we have

$$n - d \geq \frac{d}{2} + k - 2 \quad \Rightarrow \quad n \geq k + \left\lceil \frac{3}{2}d \right\rceil - 2$$

4.2 Consequences of Theorem 5

We derive from Theorem 5 a weaker version of the Griesmer bound holding for any systematic code.

Remark 1. Considering an integer d , there exist $1 \leq r < q$ and $l \geq 0$ such that

$$q^l r \leq d < q^l(r+1) \leq q^{l+1} \quad (14)$$

In particular, l has to be equal to $\lfloor \log_q d \rfloor$, and from inequality (14) we obtain $d/q^l - 1 < r \leq d/q^l$, namely $r = \lfloor d/q^l \rfloor$.

Corollary 4 (Bound A). *Let $l = \lfloor \log_q d \rfloor$ and $r = \lfloor d/q^l \rfloor$. Then*

$$S_q(k, d) \geq d + \sum_{i=1}^{k-1} \left\lceil \frac{q^l r}{q^i} \right\rceil.$$

Proof. We call s the difference between d and $q^l r$, namely $d = q^l r + s$. Note that $s \leq n - k$, and so there are at least s non-systematic coordinates. With this notation, let C be an $(n, q^k, q^l r + s)_q$ -systematic code. We build a new code C_s by puncturing C in s systematic coordinates, so that C_s has parameters $(n - s, q^k, d_s)_q$, for a certain $q^l r \leq d_s \leq q^l r + s$.

If $q^l r \neq d_s$, we can apply Lemma 1, in order to obtain another code \bar{C} , so that we have an $(n - s, q^k, q^l r)_q$ -systematic code. Due to Remark 1 it holds $1 \leq r < q$, so we can apply Theorem 5 to \bar{C} . We find $n - s \geq \sum_{i=0}^{k-1} \lceil q^l r / q^i \rceil$, hence $n \geq \sum_{i=0}^{k-1} \lceil q^l r / q^i \rceil + s$. We conclude by noticing that for $i = 0$ we have $\lceil \frac{q^l r}{q^i} \rceil = q^l r$, and by adding s we obtain exactly d . So $n \geq d + \sum_{i=1}^{k-1} \lceil q^l r / q^i \rceil$.

4.3 Consequences of Proposition 2

Next we generalize Proposition 2.

Proposition 4. *Let q, k and d be fixed, and let l be the maximum integer such that q^l divides d . Then it holds*

$$N_q(q^k, d) \geq \sum_{i=0}^h \left\lceil \frac{d}{q^i} \right\rceil,$$

where h is the minimum between $k - 1$ and l .

Proof. First, notice that $d = q^l r$, $q \nmid r$. We can use the same argument as for the proof of Proposition 2. If $k - 1 \leq l$, then we are in the same situation as above. Otherwise

$h = l$, and d is not divisible for higher powers of q , and we need to stop the sum to the term $\frac{d}{q^l}$.

Corollary 5 (Bound B). *Let q , M and d be fixed, let k the maximum integer such that $q^k \leq M$, and let l be the maximum integer such that q^l divides d . Then it holds*

$$N_q(M, d) \geq \sum_{i=0}^h \left\lceil \frac{d}{q^i} \right\rceil,$$

where h is the minimum between $k - 1$ and l .

Proof. If there exists an $(n, M, d)_q$ -code, then there exists also an $(n, q^k, d)_q$ code, due to the condition $q^k \leq M$. Hence we can apply Proposition 4.

4.4 Relations between the Griesmer bound and the Plotkin bound

We consider now the following bounds, which can be seen as weaker versions of the Griesmer bound or as an extension of the Plotkin bound.

Proposition 5. *For each choice of q , k and d , it holds*

$$N_q(q^k, d) \geq \left\lceil \sum_{i=0}^{k-1} \frac{d}{q^i} \right\rceil.$$

Proof. We can use an argument similar to the proof of Proposition 2. Suppose there is a code C such that $n < \left\lceil \sum_{i=0}^{k-1} \frac{d}{q^i} \right\rceil$. Observe that $\sum_{i=0}^{k-1} d/q^i = d \left(\frac{1-1/q^k}{1-1/q} \right) < d \left(\frac{1}{1-1/q} \right)$, i.e. $n < d \left(\frac{1}{1-1/q} \right)$, which allow us to apply the Plotkin bound and to find the contradiction $n \geq d \left(\frac{1-1/q^k}{1-1/q} \right)$.

From a direct computation, as we did in the proof, we find that Proposition 5 can be also written as

Proposition 6. *For each choice of q , k and d , it holds*

$$N_q(q^k, d) \geq \left\lceil d \left(\frac{1 - \frac{1}{q^k}}{1 - \frac{1}{q}} \right) \right\rceil. \quad (15)$$

Observe that if the code has a number of words $M \geq q^k$, then by removing $M - q^k$ codewords we obtain an $(n, q^k, d)_q$ -code and we can apply Proposition 6. We obtain the following Corollary.

Corollary 6 (Bound C). *For each choice of q , k and d , it holds*

$$N_q(N, d) \geq \left\lceil d \left(\frac{1 - \frac{1}{q^k}}{1 - \frac{1}{q}} \right) \right\rceil. \quad (16)$$

where k is the larger integer such that $M \geq q^k$.

5 Counterexamples to the Griesmer bound

In this section we show explicitly binary nonlinear codes for which the Griesmer bound does not hold. It is indeed already known that there exist pairs (k, d) for which $N_2(2^k, d) < g_2(k, d)$, however it was not clear whether the same was true for systematic codes or not. We start in the next section by expliciting a nonlinear non-systematic code whose length contradicts the Griesmer bound. Then we make use of this code to explicit a systematic code contradicting itself the Griesmer bound, proving that in general $g_2(k, d)$ is not a bound for systematic codes.

5.1 The nonlinear case

In [Lev64], Levenshtein has shown that if Hadamard matrices of certain orders exist, then the binary codes obtained from them meet the Plotkin Bound. Levenshtein's method to construct such codes can be found also in the proof of Theorem 8, of [MS77, Ch. 3, §2].

Example 1. The next code is a $(19, 16, 10)_2$ -nonlinear and non-systematic code, obtained using Levenshtein's method, as explained in [MS77, Ch. 3, §2]. All its codewords have weight 10 (except the zero codeword) and each pair of codewords has distance $d = 10$. The code is composed by the zero codeword and by 15 shifts of the codeword

$c = (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$. We show here explicitly the code:

$$C = \{(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0), \\
(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0), \\
(1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1), \\
(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1), \\
(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0), \\
(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0), \\
(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0), \\
(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1), \\
(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1), \\
(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1), \\
(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0), \\
(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1), \\
(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0), \\
(0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1), \\
(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0), \\
(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)\}$$

This code has length $n = 19 < g_2(4, 10) = 20$, i.e. the code C proves that $N_2(16, 10) < g_2(4, 10)$.

5.2 The systematic case

In this section we provide an example of an $(n, q^k, d)_2$ -systematic code for which $n < g_2(k, d)$, proving that in general the Griesmer bound does not hold for systematic codes.

Example 2. To construct an $(n, k, d)_2$ -systematic code for which $n < g_q(k, d)$, we search for a $[15, 4, 8]_2$ -linear code C_l . We remark that C_l would attain the Griesmer bound with equality, and being $d = 8$, we can apply Corollary 2 to be sure that no binary nonlinear systematic codes exists with the same dimension and distance but smaller length.

To build C_l we consider the cyclic code of length 15 associated to the complete defining set $S = \{0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 12\}$, which is a code with dimension 4 and distance 8. We can therefore find a systematic linear code equivalent to C_l . A possible choice is

the code generated by

[illegible]

To obtain a nonlinear systematic code \tilde{C} not verifying the Griesmer bound we make use of both this code and the code C in Example 1. This new code is obtained by concatenating each codeword in C_l with a different codeword in C . In this way \tilde{C} is an $(34, 4, 18)_2$ -systematic code. In the following we explicit all codewords in \tilde{C} .

[illegible]

Notice that $g_2(4, 18) = 35$, therefore $S_2(4, 18) < g_2(4, 18)$, proving that the Griesmer bound is in general not true for systematic codes.

We conjecture the following:

Conjecture 1. For any $r \geq 3$ there is a systematic code with distance $2^r + 2$ not satisfying the Griesmer bound.

The example given is a special case with $r = 4$.

6 Conclusions

In this work we have addressed the problem of characterize the Griesmer bound for systematic nonlinear codes, mainly in the binary case. The Griesmer bound is one of the few bounds which can only be applied to linear codes, however classical counterexamples arose from the Levenstein's method for building optimal nonlinear codes, which however does not provide specific counterexamples for the systematic case. It was therefore non fully understood whether the Griesmer bound would hold for systematic nonlinear codes, or whether there exist families of parameters (k, d) for which the bound could be applied to the nonlinear case. Moreover, weaker versions of the Griesmer bound might hold for nonlinear codes.

As regards nonlinear codes satisfying the Griesmer bound, the main results of our work are Theorem 6 and Corollary 3, in which we prove that whenever a binary systematic nonlinear code has a distance d such that

1. $d = 2^r$,
2. $d = 2^r - 1$,
3. $d = 2^r - 2^s$, or
4. $d = 2^r - 2^s - 1$,

then the Griesmer bound can be applied.

We also provide versions of the Griesmer bound holding for nonlinear codes: Bound A, Bound B and Bound C.

Finally, we conclude by showing explicit examples of systematic nonlinear codes for which the Griesmer bound does not hold.

All the results can be easily extended to codes over any alphabet.

7 Acknowledgements

The first three authors would like to thank their (former) supervisor: the last author.

References

- Bas65. L.A. Bassalygo, *New upper bounds for error correcting codes*, Problemy Peredachi Informatsii **1** (1965), no. 4, 41–44.
- BGS14. E. Bellini, E. Guerrini, and M. Sala, *Some bounds on the size of codes*, IEEE Trans. Inform. Theory **60** (2014), no. 3, 1475–1480.
- Del73. P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. (1973), no. 10, vi+97.

- Gol49. M. Golay, *Notes on Digital Coding*, Proc. IRE **37** (1949), 657.
- Gri60. J.H. Griesmer, *A bound for error-correcting codes*, IBM Journal of Research and Development **4** (1960), no. 5, 532–542.
- Ham93. Noboru Hamada, *A characterization of some $[n, k, d; q]$ -codes meeting the Griesmer bound using a minihyper in a finite projective geometry*, Discrete Mathematics **116** (1993), no. 1, 229–268.
- Hel81. Tor Hellesteth, *A characterization of codes meeting the Griesmer bound*, Information and Control **50** (1981), no. 2, 128–159.
- Hel92. Tor Hellesteth, *Projective codes meeting the Griesmer bound*, Discrete mathematics **106** (1992), 265–271.
- HH93. NOBORU Hamada and T Hellesteth, *A characterization of some ternary codes meeting the Griesmer bound*, Finite Fields: Theory, Applications, and Algorithms **168** (1993), 139–150.
- HP03. W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.
- Joh62. S. Johnson, *A new upper bound for error-correcting codes*, Information Theory, IRE Transactions on **8** (1962), no. 3, 203–207.
- Joh71. ———, *On upper bounds for unrestricted binary-error-correcting codes*, Information Theory, IEEE Transactions on **17** (1971), no. 4, 466–478.
- Kle04. Andreas Klein, *On codes meeting the Griesmer bound*, Discrete Mathematics **274** (2004), no. 1–3, 289–297.
- Lev64. V. I. Levenshtein, *The application of Hadamard matrices to a problem in coding*, Problems of Cybernetics (1964), no. 5, 166–184.
- Lev98. V.I. Levenshtein, *Universal bounds for codes and designs*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), vol. 1, Elsevier, 1998, pp. 499–648.
- LL98. T. Laihonon and S. Litsyn, *On upper bounds for minimum distance and covering radius of non-binary codes*, Des. Codes Cryptogr. **14** (1998), no. 1, 71–80.
- Mar96. Tatsuya Maruta, *On the non-existence of linear codes attaining the Griesmer bound*, Geometriae Dedicata **60** (1996), no. 1, 1–7.
- Mar97. ———, *On the Achievement of the Griesmer Bound*, Designs, Codes and Cryptography **12** (1997), no. 1, 83–87.
- MS77. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I and II*, North-Holland Publishing Co., Amsterdam, 1977.
- PBH98. V. Pless, R.A. Brualdi, and W.C. Huffman, *Handbook of coding theory*, Elsevier Science Inc., 1998.
- Plo60. M. Plotkin, *Binary codes with specified minimum distance*, Information Theory, IRE Transactions on **6** (1960), no. 4, 445–450.
- SS65. G. Solomon and J. J. Stiffler, *Algebraically punctured cyclic codes*, Information and Control **8** (1965), no. 2, 170–179.
- Tam84. Fumikazu Tamari, *On linear codes which attain the Solomon-Stiffler bound*, Discrete Mathematics **49** (1984), no. 2, 179–191.

- Tam93. ———, *A construction of some $[n, k, d; q]$ -codes meeting the Griesmer bound*, Discrete Mathematics **116** (1993), no. 1–3, 269–287.
- Van80. Henk Van Tilborg, *On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound*, Information and control **44** (1980), no. 1, 16–35.
- War98. Harold N Ward, *Divisibility of codes meeting the Griesmer bound*, Journal of Combinatorial Theory, Series A **83** (1998), no. 1, 79–93.
- ZL84. V. A. Zinov'ev and S.N. Litsyn, *On Shortening of Codes*, Problemy Peredachi Informatsii **20** (1984), no. 1, 3–11.